(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
7 novembre 2002 (07.11.2002)

PCT

(10) Numéro de publication internationale
WO 02/088934 A1

(51) Classification internationale des brevets⁷ : G06F 7/72

(21) Numéro de la demande internationale :
PCT/FR02/01491

(22) Date de dépôt international : 29 avril 2002 (29.04.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/05815 30 avril 2001 (30.04.2001) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **STMICROELECTRONICS S.A.** [FR/FR]; 29, boulevard Romain Rolland, F-92120 Montrouge (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **LIARDET, Pierre-Yvan** [FR/FR]; 56, rue du Pralou, Lotissement L'Audiguier, F-13790 Peynier (FR). **ROMAIN, Fabrice** [FR/FR]; Les Héliades, Bât. A, 535, avenue de Bagatelle, F-13090 Aix en Provence (FR).

(74) Mandataire : **DE BEAUMONT, Michel**; Cabinet Michel de Beaumont, 1, rue Champollion, F-38000 Grenoble (FR).

(81) États désignés *(national)* : JP, US.

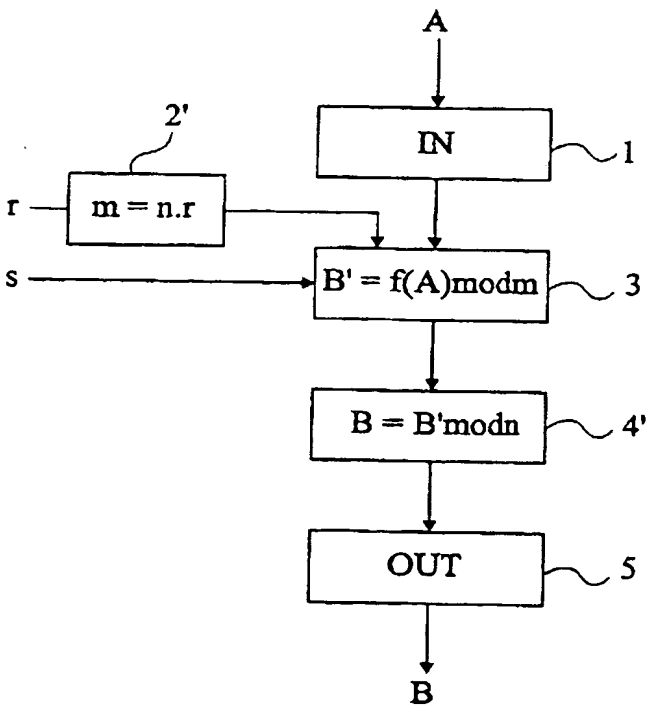
(84) États désignés *(régional)* : brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Publiée :
— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: METHOD FOR ENCRYPTING A CALCULATION USING A MODULAR FUNCTION

(54) Titre : BROUILLAGE D'UN CALCUL METTANT EN OEUVRE UNE FONCTION MODULAIRE



(57) **Abstract:** The invention concerns a method for encrypting, with a random quantity (r), a calculation using at least a modular operation (3), the method consisting in multiplying a first modulo (n) by said random quantity, in taking as modulo of the operation, the result (m) of said multiplication and in carrying out a modular reduction of the result of the operation, on the basis of the first modulo (n).

(57) **Abrégé** : L'invention concerne un procédé de brouillage, au moyen d'une quantité aléatoire (r), d'un calcul mettant en oeuvre au moins une opération modulaire (3), le procédé consistant à multiplier un premier modulo (n) par ladite quantité aléatoire, à prendre comme modulo de l'opération, le résultat (m) de cette multiplication et à effectuer une réduction modulaire du résultat de l'opération, sur la base du premier modulo (n).

WO 02/088934 A1

BROUILLAGE D'UN CALCUL METTANT EN OEUVRE UNE FONCTION MODULAIRE

La présente invention concerne la protection d'une clé ou donnée secrète (mot binaire) utilisée dans un processus d'authentification ou d'identification d'un circuit électronique (par exemple, une carte à puce) ou analogue, contre des tentatives de piratage. L'invention concerne plus particulièrement le brouillage des calculs prenant en compte la donnée secrète. Par brouillage, on entend une modification des caractéristiques physiques observables (consommation, rayonnements thermique, électromagnétique, etc.) induites par le fonctionnement d'un composant.

Un exemple d'application de la présente invention concerne un processus de contre-mesure contre une attaque par analyse de la consommation directe (Simple Power Analysis, SPA) ou statistique (Differential Power Analysis, DPA) d'un circuit de traitement numérique exploitant une donnée privée ou secrète. Une telle attaque par analyse de la consommation constitue une attaque susceptible d'être utilisée aujourd'hui par des pirates pour tenter de découvrir une clé numérique ou analogue. Une telle attaque consiste à évaluer la dépendance directe ou statistique entre la consommation du circuit et l'utilisation de données numériques traitées par une puce et faisant intervenir une quantité secrète. En effet, dans un traitement algorithmique

au moyen d'un circuit de traitement, il existe une dépendance entre la consommation du circuit et la donnée traitée. Le pirate utilise la ou les données introduites dans le circuit, donc "visibles", et utilisées par l'algorithme, afin de déterminer la donnée secrète enfouie dans le circuit, en examinant sa consommation lors de l'exécution de l'algorithme.

Afin de rendre plus difficile les attaques par analyse différentielle de consommation, on cherche généralement à rendre indépendantes les données visibles des données traitées. Par données visibles, on entend les mots binaires introduits dans le circuit de traitement algorithmique et extraits de ce circuit. Le calcul proprement dit, qui influence le plus la consommation du circuit, s'effectue alors sur une donnée modifiée ou brouillée.

Généralement, on utilise une valeur aléatoire pour convertir la donnée introduite en une donnée brouillée participant au calcul.

La figure 1 représente, sous forme d'organigramme très schématique, un exemple classique de procédé de traitement d'une donnée A introduite dans une puce d'authentification par un algorithme de calcul réalisant une opération modulaire. L'introduction de la donnée A est symbolisée en figure 1 par un bloc 1 (IN). La donnée A est ensuite convertie en une donnée A' (bloc 2) en utilisant une quantité aléatoire r. Cette conversion consiste, par exemple, à appliquer une opération arithmétique aux opérandes A et r. La donnée A' subit le calcul de la fonction d'authentification (bloc 3). Ce calcul consiste à effectuer une opération $B' = f(A')$ modulo n, où la fonction f représente une opération arithmétique modulaire. La taille (nombre de bits) du modulo n de cette fonction est généralement prédéterminée par le nombre de bits pour lequel est prévu le circuit de traitement. En effet, on dimensionne généralement le nombre de bits sur lesquels sont exécutées les opérations en fonction des moduli utilisés par ces opérations et des tailles maximales des opérandes et résultats.

Dans l'application plus particulière de l'invention à un traitement d'un algorithme mettant en jeu une donnée secrète s, cette donnée est contenue dans la puce (par exemple, enregistrée à demeure) et est fournie à l'algorithme lors de l'opération de calcul (bloc 3). C'est cette donnée secrète que cherche à détecter le pirate par une analyse de la consommation. Sans le brouillage de la donnée A en donnée A', ce piratage éventuel est facilité dans la mesure où le pirate connaît la donnée A introduite ainsi que le modulo n de la fonction modulaire.

Un exemple courant de fonction arithmétique modulaire est l'exponentiation modulaire qui consiste à appliquer la formule suivante :

$$B' = A'^{S} \text{ modulo } n.$$

Une fois le résultat B' obtenu par la mise en oeuvre de l'algorithme de calcul, ce résultat est converti, de façon inverse, pour restituer une donnée B (bloc 4) qui est fournie (bloc 5, OUT), en sortie du circuit. La quantité aléatoire r doit être mémorisée (bloc 6, MEM) entre les étapes 2 et 4, afin d'être réutilisée lors de la conversion inverse appliquée au résultat de l'algorithme.

Un inconvénient des procédés de brouillage classiques mettant en oeuvre l'opérande de l'algorithme est qu'ils requièrent une puissance de calcul supplémentaire par rapport à la simple exécution de l'algorithme. En particulier, la conversion de B' en B requiert autant de ressources (mémoire, temps de calcul, etc.) que le calcul de la fonction même.

Un autre inconvénient des procédés classiques est que la mémorisation de la quantité aléatoire r fragilise le processus de contre-mesure à une attaque par examen de la consommation du circuit.

En outre, le simple fait de devoir mémoriser cette donnée aléatoire requiert des circuits spécifiques prenant de la place supplémentaire.

Le document EP-A-1 006 492 décrit un procédé de calcul mettant en oeuvre une opération modulaire dans lequel une quantité aléatoire est réutilisée en fin de procédé. Cela nécessite donc la mémorisation de la quantité aléatoire.

Le document WO-A-98 52319 décrit également un procédé de calcul faisant intervenir une quantité aléatoire. Cette quantité intervient dans le modulo de l'opération et doit également être mémorisée.

La présente invention vise à proposer une nouvelle solution pour brouiller un calcul mettant en jeu au moins une opération arithmétique modulaire, qui nécessite moins de ressources de calcul que les solutions classiques, et qui évite la mémorisation, pendant toute la durée du calcul, d'une quantité aléatoire intervenant dans le brouillage.

Pour atteindre ces objets et d'autres, la présente invention prévoit un procédé de brouillage, au moyen d'une quantité aléatoire, d'un calcul mettant en oeuvre au moins une opération modulaire, consistant à multiplier un premier modulo par ladite quantité aléatoire, à prendre comme modulo de l'opération, le résultat de cette multiplication, et à effectuer une réduction modulaire du résultat de l'opération, sur la base du premier modulo.

Selon un mode de réalisation de la présente invention, ladite opération met en oeuvre au moins une donnée d'entrée ainsi qu'au moins une donnée secrète.

Selon un mode de réalisation de la présente invention, ladite donnée secrète est contenue dans un circuit électronique mettant en oeuvre le procédé.

Selon un mode de réalisation de la présente invention, ladite donnée d'entrée est une donnée introduite dans un circuit électronique mettant en oeuvre le procédé.

L'invention prévoit également un circuit de traitement mettant en oeuvre ce procédé.

Ces objets, caractéristiques et avantages, ainsi que d'autres de la présente invention seront exposés en détail dans

la description suivante de modes de mise en oeuvre et de réalisation particuliers faite à titre non-limitatif en relation avec les figures jointes parmi lesquelles :

la figure 1 illustre sous forme d'organigramme simplifié, la mise en oeuvre d'un procédé de calcul mettant en oeuvre une donnée externe brouillée selon l'état de la technique ; et

la figure 2 illustre, par un organigramme très schématique, un mode de mise en oeuvre du procédé de brouillage selon la présente invention.

Les mêmes éléments sont désignés par les mêmes références aux différentes figures. Pour des raisons de clarté, seules les étapes du procédé de brouillage et de calcul qui sont nécessaires à la compréhension de l'invention ont été illustrées aux figures et seront décrites par la suite. En particulier, les traitements affectant les données n'ont pas été détaillés et ne font pas l'objet de la présente invention. Celle-ci s'applique quels que soient les traitements aval et amont effectués.

La figure 2 illustre, par un organigramme simplifié à rapprocher de celui de la figure 1, un mode de mise en oeuvre du procédé selon l'invention.

Une caractéristique de la présente invention est de brouiller, non plus l'opérande A introduit de l'extérieur (bloc 1, IN), mais le modulo de l'opération arithmétique modulaire réalisée.

Ainsi, selon la présente invention, pour une fonction modulaire de modulo n, on tire à chaque calcul, un nombre entier aléatoire r et l'on multiplie ce nombre aléatoire (bloc 2') au modulo n. On obtient alors un nombre m qui, selon l'invention, est utilisé comme modulo du calcul d'authentification (bloc 3). Ce calcul met donc en oeuvre directement l'opérande A et le modulo modifié m. L'opération mise en oeuvre n'est pas modifiée par rapport au cas classique. Toutefois, on voit bien qu'en affectant le modulo de l'algorithme d'authentification, on affecte les valeurs respectives, donc la consommation du circuit. L'objectif de brouiller le calcul est donc atteint.

Le résultat B' = f(A) modulo m doit, comme c'était le cas précédemment (bloc 4, figure 1), être converti de façon inverse.

Toutefois, selon l'invention, cette conversion inverse (bloc 4', figure 2) est particulièrement simple. En effet, comme le modulo m employé dans l'opération modulaire est un multiple de n (m = r . n), il suffit de réduire le nombre B' modulo n pour obtenir le résultat B à fournir (bloc 5, OUT) en sortie du circuit.

Un avantage de la présente invention est qu'une telle réduction modulaire n'engendre que peu de calculs de même que l'opération multiplicative du modulo.

Un autre avantage de l'invention est qu'il n'est plus nécessaire de mémoriser la quantité aléatoire r pour la conversion inverse. On peut alors effacer cette quantité aléatoire r dès que le nombre m a été calculé (bloc 2'). On rend encore plus difficile le piratage éventuel de la donnée secrète s intervenant dans le calcul.

Le brouillage ou masquage effectué selon l'invention est particulièrement simple à réaliser. On doit simplement tenir compte du nombre de bits pris en compte dans les opérations avec le modulo de plus grande taille, pour dimensionner les circuits de traitement des nombres.

Par exemple, pour un circuit de traitement effectuant classiquement une opération modulaire sur 1024 bits, on peut prévoir d'ajouter 64 bits au nombre traité. Les 64 bits représentent la taille de la quantité aléatoire r mise en oeuvre.

Dans une application particulière de l'invention à une exponentiation modulaire, celle-ci présente un avantage particulier en simplifiant considérablement les calculs par rapport au traitement classique de l'opérande. En effet, une exponentiation modulaire est généralement mise en oeuvre par une technique parfaitement connue de carré-multiplication qui consiste à opérer autant de carrés modulaires que le nombre de

bits de l'exposant et autant de produits que le nombre de bits à l'état 1 que comporte l'exposant.

Bien entendu, la présente invention est susceptible de diverses variantes et modifications qui apparaîtront à l'homme de l'art. En particulier, on pourra choisir des dimensions quelconques pour les nombres n et r. On effectuera généralement un compromis entre la taille du modulo et la taille de la quantité aléatoire. En pratique, la taille du modulo est souvent fixée par des impératifs externes (normes, etc.). On accroît alors légèrement (selon la taille choisie pour la quantité aléatoire) le nombre de bits traités par le circuit.

De plus, le procédé de l'invention pourra être combiné au procédé classique pour des applications où l'on est prêt à sacrifier du temps de calcul pour accroître le brouillage.

En outre, on notera que l'invention s'applique plus généralement à n'importe quelle fonction modulaire (par exemple, addition, soustraction, multiplication, inversion modulaire, etc.) et quels que soient les nombres de fonctions calculées et de données d'entrée/sortie, sa mise en oeuvre étant à la portée de l'homme du métier à partir des indications fonctionnelles données ci-dessus. On pourra se référer, par exemple, à l'ouvrage "Handbook of Applied Cryptography" de A.J. Menezes, P.C. van Oorschot et S.A. Vanstone, paru en 1997 aux éditions CRC Press LLC (pages 297, 454 à 459 et 484) pour des exemples d'algorithmes dits d'ELGAHAL et dérivés, mettant en oeuvre des opérations modulaires, auxquels s'applique l'invention.

Enfin, la réalisation d'un circuit de traitement mettant en oeuvre le procédé de calcul et de brouillage de l'invention est à la portée de l'homme du métier à partir des indications fonctionnelles données ci-dessus. La mise en oeuvre de l'invention ne requiert que des moyens classiques, qu'il s'agisse d'une mise en oeuvre logicielle par un microcontrôleur ou d'une mise en oeuvre matérielle par une machine d'états en logique câblée. L'invention qui a été décrite ci-dessus en faisant référence à des exemples de tailles de nombres indiquées

sous forme de bits pourra, bien entendu, être transposée à d'autres bases, pourvu que les moyens de calcul utilisés acceptent de telles bases.

REVENDICATIONS

1. Procédé de brouillage, au moyen d'une quantité aléatoire (r), d'un calcul mettant en oeuvre au moins une opération modulaire (3), caractérisé en ce qu'il consiste :

à multiplier un premier modulo (n) par ladite quantité aléatoire ;

à prendre comme modulo de l'opération, le résultat (m) de cette multiplication ; et

à effectuer une réduction modulaire du résultat de l'opération, sur la base du premier modulo (n).

2. Procédé selon la revendication 1, caractérisé en ce que ladite opération (3) met en oeuvre au moins une donnée (A) d'entrée ainsi qu'au moins une donnée secrète (s).

3. Procédé selon la revendication 2, caractérisé en ce que ladite donnée d'entrée (A) est une donnée introduite dans un circuit électronique mettant en oeuvre le procédé.

4. Procédé selon la revendication 2 ou 3, caractérisé en ce que ladite donnée secrète (s) est contenue dans un circuit électronique mettant en oeuvre le procédé.

5. Circuit de brouillage d'un calcul réalisé par un circuit intégré, caractérisé en ce qu'il comprend des moyens pour mettre en oeuvre le procédé selon l'une quelconque des revendications 1 à 4.

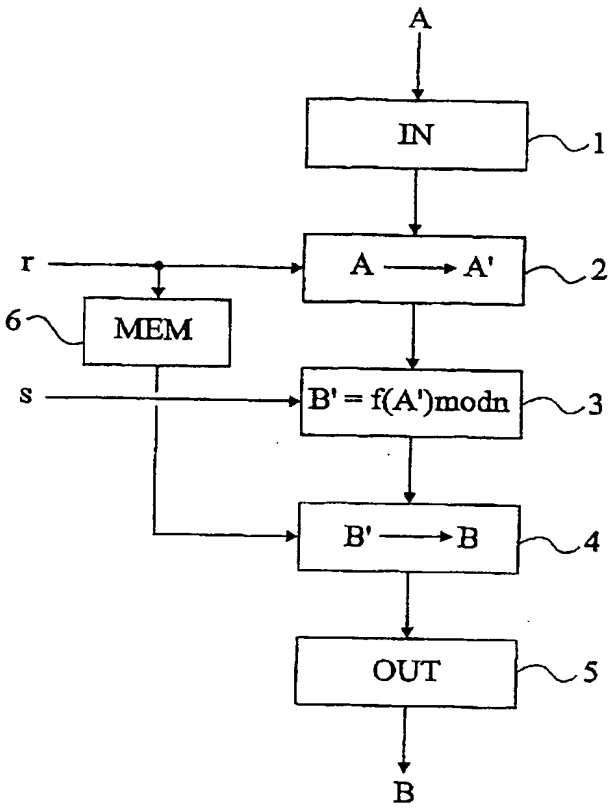

A
IN
1
r
A → A'
2
6
MEM
s
B' = f(A')modn
3
B' → B
4
OUT
5
B

Fig 1

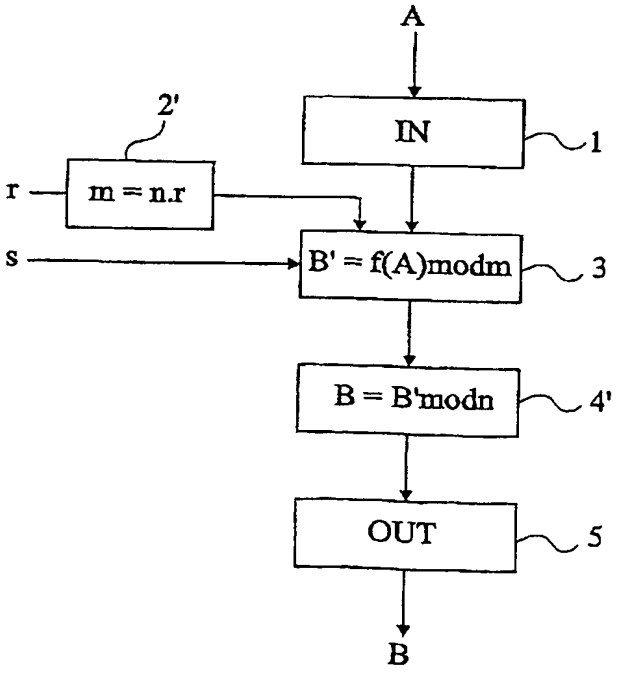

A
2'
IN
1
r
m = n.r
s
B' = f(A)modm
3
B = B'modn
4'
OUT
5
B

Fig 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 02/01491

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 006 492 A (HITACHI LTD) 7 June 2000 (2000-06-07) paragraph '0084! - paragraph '0089!; figure 31	1-5
X	WO 98 52319 A (YEDA RES & DEV ;FLEIT LOIS (US)) 19 November 1998 (1998-11-19) page 12, line 6 -page 13	1-5
A	WO 99 35782 A (CRYPTOGRAPHY RESEARCH INC) 15 July 1999 (1999-07-15) figure 3	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 August 2002	22/08/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Verhoof, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

nformation on patent family members

International Application No
PCT/FR 02/01491

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 1006492	A	07-06-2000	JP	2000165375 A	16-06-2000
			CN	1255692 A	07-06-2000
			EP	1006492 A1	07-06-2000
			TW	466393 B	01-12-2001
			US	6408075 B1	18-06-2002
WO 9852319	A	19-11-1998	US	5991415 A	23-11-1999
			AU	7568598 A	08-12-1998
			EP	0986873 A1	22-03-2000
			WO	9852319 A1	19-11-1998
WO 9935782	A	15-07-1999	AU	2557399 A	26-07-1999
			CA	2316227 A1	15-07-1999
			EP	1050133 A1	08-11-2000
			WO	9935782 A1	15-07-1999
			US	6304658 B1	16-10-2001
			US	2001002486 A1	31-05-2001

RAPPORT DE RECHERCHE INTERNATIONALE

D e Internationale No
PCT/FR 02/01491

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F7/72

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 1 006 492 A (HITACHI LTD) 7 juin 2000 (2000-06-07) alinéa '0084! - alinéa '0089!; figure 31	1-5
X	WO 98 52319 A (YEDA RES & DEV ;FLEIT LOIS (US)) 19 novembre 1998 (1998-11-19) page 12, ligne 6 -page 13	1-5
A	WO 99 35782 A (CRYPTOGRAPHY RESEARCH INC) 15 juillet 1999 (1999-07-15) figure 3	1

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
15 août 2002	22/08/2002

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Verhoof, P

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relat membres de familles de brevets

D e internationale No
PCT/FR 02/01491

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 1006492	A	07-06-2000	JP	2000165375 A	16-06-2000
			CN	1255692 A	07-06-2000
			EP	1006492 A1	07-06-2000
			TW	466393 B	01-12-2001
			US	6408075 B1	18-06-2002
WO 9852319	A	19-11-1998	US	5991415 A	23-11-1999
			AU	7568598 A	08-12-1998
			EP	0986873 A1	22-03-2000
			WO	9852319 A1	19-11-1998
WO 9935782	A	15-07-1999	AU	2557399 A	26-07-1999
			CA	2316227 A1	15-07-1999
			EP	1050133 A1	08-11-2000
			WO	9935782 A1	15-07-1999
			US	6304658 B1	16-10-2001
			US	2001002486 A1	31-05-2001